Global Information Assurance Certification Paper

INTELLECTUAL PROPERTY: PROTECTION, DETECTION, AND REMEDIATION

SANS GCIH PRACTICAL V2.1
SPECIAL APPROVED ASSIGNMENT

by

GREG JONES
MARCH 2003

ABSTRACT

This document will discuss some of the aspects related to incidents involving intellectual property (IP). Specifically, there will be three areas of importance addressed. The first area is the protection of IP and other confidential information. This will be followed by a section which discusses the detection of an IP incident. Finally, the section labeled *Remediation* will begin to introduce some of the steps involved in remedying an IP misuse. In this document an IP misuse is used to identify such acts as stealing, copying, modifying, destroying, plagiarizing, or displaying IP in a manner which may be illegal and directly or indirectly harmful to the IP owner. Most of the IP specific content and examples were obtained while I served as a member of an IP Incident Response Team for the SANS Institute.

INTRODUCTION

Over the past few decades, digital information has become an increasingly important part of our world including areas such as the advancement of medical and scientific research, as well as the world economy. As our world continues to progress forward into the digital age, the bottom line value for business is becoming more driven from intellectual assets. Intellectual assets are non-tangible assets, such as confidential information like software code, strategies, methodologies, and processes which are crucial in the effective operations and the development of goods and services of an organization. These intellectual assets can be a key to the success of many organizations such as militaries, governments, and corporate businesses. Intellectual properties are intellectual assets in which the owners have taken legal steps to protect via such means as copyrights, patents and trademarks. Intellectual property (IP) can present some challenging obstacles for its defender. One reason is that IP can be represented in a digital format. Examples include software, music, video, and documentation. Due to the fact that digital IP is such an important asset to many organizations, it is vital to have mechanisms in place to protect IP, detect its misuse, and remedy these misuses.

PROTECTION

There are three primary methods for protecting IP: physical, technical, and legal. All three are very important and the owner should not feel that one method can replace another. Although there is enough information within each of these three areas to fill a paper on their own, I will briefly touch upon only a few aspects in each area.

Physical Protection

There are three areas of physical protection I want to mention: physical access, backups and awareness. Physical protection of the IP originals should follow standard physical security and disaster recovery guidelines.

Physical Access

The most basic physical security protection is ensuring that physical access to the IP is restricted to authorized personnel. Verify that proper physical access controls are installed and operational. These controls need to uniquely identify the individual and the dates and times of each access. This information must be recorded and maintained in detailed logs. These logs need to be distributed to the appropriate auditors for review. These last steps are extremely beneficial in curbing insider corporate espionage and theft of IP.

Physical Backups

Although backups may be technical in nature, I choose to mention them as a physical protection. It is important that while developing protection strategies to not only be protecting from unauthorized access and theft, but also protecting against accidental or malicious destruction or modification. Proper backups and secure backup storage are the most fundamental steps taken to provide this

base level of physical protection. Perform appropriate backups often. This means that much thought should go into whether complete daily backups or incremental daily backups with complete weekly backups are needed. Additionally, make sure to test the backup restoration process. Quick access should be available to these backups as well as to additional hardware and necessary operating system and application software. If backups are performed across the network, verify that there is a secure connection or that the backup tool utilizes some form of strong encryption. Otherwise, any network sniffer will be able to compromise the confidentiality of your IP.

Physical Awareness

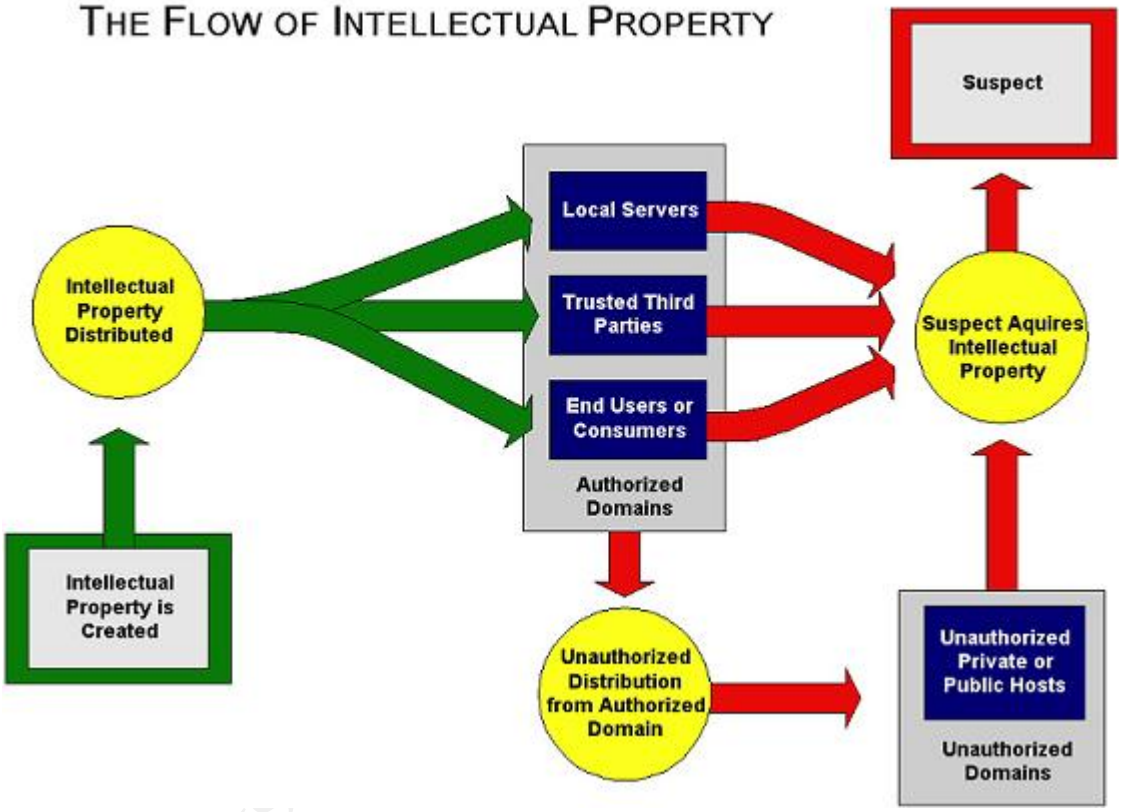
Another simple but often overlooked physical protection is physical awareness. The first goal is to pay attention to people or things that do not fit. This is one advantage to departmental and organizational events. It allows people to identify who belongs. This will subconsciously prepare them to quickly spot those who do not belong. As part of your organizations security strategy, all levels of employees need to be encouraged to take notice and question people who do not belong. Be aware to the presence of a lone laptop sitting on someone's desk. Network administrators frequently rely on ACLs (Access Control Lists), domain controllers, or other host or network applications to provide for *all* of the security. However, a lone laptop on a disgruntled employee's desk can circumvent these access control mechanisms and be used to steal all sorts of trade secrets or IP as it traverses your network. Administrators should take the responsibility to implement detection measures to identify any rogue devices. These detection measures may be automated, manual, or a combination of both methods. For example, in addition to employing network management tools to identify and map network devices, administrators may occasionally walk around in an attempt to identify unauthorized hardware (e.g. laptops, modems, CD burners). The next aspect of physical awareness is to pay attention to people's habits which may be out of the ordinary. Do you notice an employee who was just passed over for promotion spending unusually long hours working late? Do your access logs identify them coming in on the weekends unexpectedly? Of course, there may be perfectly reasonable explanations for this; however, it may pay to observe these people more closely.

Technical Protection

Host Protection, File Protection, and *Network Protection* are the three areas that will be addressed in the area of technical protection. Technical protection of IP should follow standard and proven guidelines for host, file, and network systems where the IP resides and travels. Stay current on what works and what does not work through various informational sources. One excellent source of information is the SANS web site (http://www.sans.org/). On their site they offer an excellent array of courses, online documentation including a comprehensive reading room (http://www.sans.org/rr/). Another source is the Security Focus web site (http://www.securityfocus.com/).

Host Protection

The first course of action is to make certain that the hosts where the IP resides are protected. This is where the real obstacles begin to present themselves. How do we identify the hosts to secure and how do we secure them once we identify them? Let us take a moment to identify where IP can reside. The following diagram is a simplified approach used to identify at a macro level where IP may be found throughout its lifetime. It also identifies common paths to the misuse of IP by a suspect. Here, the term *suspect* is used to identify the individual misusing the IP.



We can see that once IP is created it is stored in authorized domains. This may include internal file servers, trusted third parties (e.g. resellers and distributors), or end users (e.g. consumers, subscribers, and readers). Due to ownership and close proximity, the local servers will afford the best opportunity for defense. This should include current and reliable virus protection and host level file, operating system and network access control mechanisms. Depending on the overall organization's information security strategy, host intrusion detection systems (IDS) or a host firewall may be appropriate. Consider file system encryption if the host contains extremely sensitive IP or other confidential information. The next authorized domain member to consider is trusted third parties. This is where strong business policies and practices will help leverage

the securing of these more remote hosts. Ensure during the negotiation and contractual phases that proper host and network security requirements are guaranteed by the third party. Also establish a method for auditing these security features. The final authorized domain category is the end user. Think of how many millions of dollars are lost each year by music and movie consumers making illegal copies for themselves or others. How do the owners protect against these illegal copies? To date this remains an unanswered question as a multitude of efforts have failed to provide adequate protection. We have seen recently in the news the story of how manufactures such as Sony implemented a mechanism to prevent the copying of CDs through the use of encoded data on the CD media. However, we have also seen the easy circumvention of this safeguard with an inexpensive felt tip marker. For now, protection of IP at the end user level will have to rely on legal means and detection schemes to protect and identify illegal copies of IP.

File Protection

The first file level protection guideline that must be followed is to use strong encryption mechanisms on the IP. Encryption protects IP at the file level by making the digital data unrecognizable through various manipulations of the data. This manipulation is usually performed by logical or mathematical algorithms applied to the raw binary data. Only individuals with the proper password or pass phrase will be able to access the file through a process called decryption which restores the encrypted file into its original form. At a bare minimum, use current encryption technology if IP must traverse public networks or third-party private networks. However, ideally IP will be encrypted while it is stored as well as in transit. Pretty Good Privacy (PGP) is a standard encryption mechanism. There are freeware versions and commercial versions available at http://www.pgp.com. Other commonly used encryption algorithms include Blowfish, AES, and Triple DES. Access control is an extremely important aspect of file protection. Ensure that proper file permissions are applied, maintained, and managed. Another fairly obvious but just as important file level protection is to properly identify and document the file. Titles, authors and IP contents should be documented thoroughly. An additional option to consider is creating IP in read-only formats with password protection prior to its distribution. For example, if the IP is a document, consider generating it in a format such as PDF. PDF generators such as Adobe Acrobat (http://www.adobe.com/acrofamily/main.html) have the ability to generate read-only formats that eliminate the ability to cut and paste text from one document to the next. Although this defense is not impenetrable, it does offer one more layer of protection against accidental or malicious modification or other types of misuse. After the IP is in a read-only format, be sure to capture file signatures utilizing hash algorithms like MD5 or SHA-1. Hash algorithms offer a way to "fingerprint" a file by generating a unique fixed length value. This value can be used later in various detection mechanisms and in the identification phase of the incident handling process.

Network Protection

Network protection from the perspective of IP should follow standard network security practices. Invest in a properly architected network security strategy. Secure the perimeters by installing properly configured firewalls. Install network intrusion detection to help assist in recognizing and alarming when an attack occurs. Once a sound network strategy has been implemented, have reputable professional teams perform penetration testing and vulnerability assessments. Although there are other fundamental network security strategies that can be applied, the final one I wish to mention is to use secured connections. In this manner, if someone is to successfully breach your network or transmission path, a properly secured connection will keep your valuable IP and other information confidential. For additional information, refer to the SANS Institute's *Firewalls, Perimeter Protection and VPNs* course.

Legal Protection

Recall that IP are intellectual assets which have legal protections. Thus, legal protections are what truly define IP. In most cases, the legal protections are what will win a civil or criminal case. Four of the most well known legal protections are copyrights, patents, trademarks and licensing. A copyright affords to the owner of the material authorship rights. This means that other individuals or organizations cannot copy, display, perform or sell the material. Additionally, it restricts others from deriving new material based on the original material. This last point has flooded the news in recent months as aspiring writers and authors attempt to create their own works based off the work of previous artists or authors. The Eldred case (http://reason.com/links/links011703.shtml) is an excellent example of the current state of affairs that could have had a major impact on the profits of such companies like Disney. Copyrights can be registered through the United States Copyright Office of the Library of Congress. A link to the web site has been included in the *Resource* section at the end of this document. It is important to clearly label your copyrighted material with a copyright notice as this will strengthen your court case. However, just because IP is not labeled with a copyright notice does not mean it is not protected by copyright law. Many people have found this out the hard way as they illegally posted protected materials on their web site. While a copyright can prevent others from copying the presentation, style and organization of IP material, a patent protects the owner of an invention. An invention can include things like an object, device, or design. A patented invention is protected from being imported, made, used, or sold by entities other than the owner. Notice I said *imported*. This is because patents only apply within the nation where they are applied. So, if you have a great invention, you better start applying for patents in more than your home country. A US patent can be applied for through the United States Patent Office. A trademark protects words and/or symbols. Identifying marks such as logos or names can be protected by trademarks. Interestingly, the word *Laundromat* is the name of one of the first clothes washing businesses. Since the word was not trademarked it is now used everywhere by everyone. Nike, Pepsi and Coke are just a few of the more well known trademarks. In the United States, trademarks

can be applied for at the state level or the federal level depending on the organization's needs. Licensing is another important legal protection as well as a possible additional stream of income. Licensing is frequently used to bind the user to a specific set of allowable actions that the user may perform with the IP. Anyone familiar with purchasing software is aware of costly license fees. Licensing spells out exactly what individuals and organizations may and may not do with your IP. With any of these legal protections, always consult with qualified and experienced legal counsel.

That concludes this brief discussion on physical, technical and legal IP protections. However, it is worthy to mention that a strategy or process is really needed to help unify these three protections. One such example is to have an IP management process.

IP Management Process

An IP management process is a methodical and formal set of policies and procedures for maintaining proper control of IP. Design the process to custom fit the organization's unique IP and environment. The following paragraph will identify a few considerations to follow during the development of an IP management process.

It is important to have an IP management process in place to help ensure that the physical, technical and legal protections are implemented at the proper moments during the lifetime of IP. This process will help in such tasks as maintaining rigid control over who has access, when they accessed it and where IP is stored. Depending on the size of the distribution and resources available, it may be wise to include procedures that allow for unique identification of IP as it is distributed to various sources. This can be compared to batch numbers on various food and drugs. If an illness occurs from a particular food or drug, then it may be possible to identify the distribution plant via a batch number during the investigations. Likewise, if IP is found being illicitly sold on the Internet, wouldn't it be nice if the IP contained a hidden code or phrase that would identify from which end user or third party it was taken? Here are some other questions to consider: Have the copyrights, patents or trademarks been registered? Are there secure offsite backups of the IP originals? Have you documented the creators and modifiers of IP? If the IP is confidential, who has touched the IP over its lifetime? Where has the IP been distributed? Are third parties properly securing your IP? These are just a few of the questions which will be easy to answer if a proper management process is implemented. Another important aspect of the management process should be system and process audits. The security of a system is not known without frequent audits. This applies to all levels of protection discussed to this point. Perform audits of the IP during its creation to ensure that it is properly secured while it is in the development phases. This may include checking to make sure hard copies of confidential information or specification guidelines are not left out on desks for unauthorized individuals to see or steal. Corporate espionage can easily be carried out by

temporarily filling the role of the night office cleaning person who frequently has keys to most offices. They can acquire all kinds of valuable IP from the tops of desks, unlocked drawers or even the trash. So take the few extra moments to put it away, lock it up, and shred when necessary. Continue to perform audits of the IP management process and systems on a regular basis. A final aspect of the management process I will mention is the need to assign value to IP. When you contact the FBI or an attorney because someone is misusing your IP, one of the first questions they will ask is "How much is it worth?" or "How much was the damage?" When an incident occurs, law enforcement and legal counsel will need to know this information. There are many companies and excellent publications on IP that can guide you in your effort to determine this value.

DETECTION

There are two realms in which IP owners should have detection mechanisms: internally and externally. Although the media tends to focus on external "hacker" attacks on organizations' information systems, according to many recent studies, internal employees are the biggest threat to computer and network resources. These insider breaches can give unauthorized individuals direct access to IP. As discussed earlier, the IP management process ensures that proper policies and procedures are being applied to IP which in turn provide protection. This process allows IP owners to know where IP is being created, stored and deployed. This information can be used to set up detection mechanisms at key locations during the lifetime of IP. If a particular file server is being used to store IP during the development phase, then it may be wise to establish a network packet filter in the path to ensure only authorized internet protocol addresses of developers are allowed access. Additionally, it may be possible to configure an IDS system such as Snort (http://www.snort.org) to track the movement of files from this server. Any file downloads with packets fitting the applied IDS signatures could then trigger an alarm to an incident response team as appropriate. Additional content checking may be applied on corporate email servers as well as perimeter firewalls. If the majority of firewall traffic for your organization is web content and file downloads, then a group of PDF files leaving your organization may be cause for suspicion. This is where proper traffic analysis baselines will prove valuable. Organizations need to know what is considered "normal" traffic for their networks. This will aid in the development of IDS signatures as well as identifying obtuse information in your firewall logs. Another valuable key is having experienced individuals reviewing various system and IP audit and access logs. These logs need to identify physical as well as electronic access to the IP.

This illustrates a couple of ways to identify possible IP intrusions internally. However, what if an intrusion has escaped detection or if an end user is making illegal copies of IP? How can these types of incidents be detected? It depends on how the IP is misused. For example, if school kids are making copies and physically distributing them in class, then it will be hard to detect unless someone steps forward with incriminating information. On the contrary, if the IP is distributed or sold from an illegal web site, then there may be hope in detecting it.

One very successful method for detecting the latter example of misuse is utilizing public search engines such as Google (http://www.google.com) to do internet lookups. A search engine is an extremely valuable detection and investigation tool. During the protection section, it was suggested to track information such as title, author, and content for each IP. This information can now be used to generate keyword searches for IP within search engines. As part of a current research effort in the area of IP, SANS has recently identified many illegal copies of its IP across the Internet using this very method and is now researching civil, criminal and other approaches against the suspect individuals and organizations. Additionally, there are firms for hire which can perform various types of IP searches. Go to your favorite search engine and search on the phrase "intellectual property detection service". Most of the services available are advertised for educational faculty to use in order to detect when students may be plagiarizing assignments; however, this field may become expanded in the near future as digital dependent companies strive to protect their IP assets. Another interesting resource is Googlert (http://www.googlert.com/). It will automatically check for of the presence of information on the Internet.

Although there are no hard and fast rules for detecting IP externally, such as on the Internet, there is a logical set of steps which can be used as a guide to get started:

1. Identify the IP. Ideally, this will be a preparatory step. Essentially, this means to list and document IP. This should include titles, subtitles, authors, and abstracts. Additionally, identify key phrases that may be unique to the organization or IP. For example, a key phrase for SANS may be "Copyright 2003, The SANS Institute".
2. Focus detection efforts. In other words, for what are we searching? Music, whitepapers, or videos? This is important because it may help to dictate the best place to search.
3. Identify target realm to search. Theoretically, the target realm may be the Internet, or in other cases, the target realm may be a smaller private network or group of networks or even a single host. For SANS, the target realm at this stage is primarily the Internet.
4. Identify the tools and strategies for searching the target realm. This is dependent on the two previous steps: *Focus detection efforts* and *Identify the target realm to search*. To intelligently pick the proper search tool, it is important to determine what type of IP is trying to be detected and where it will be detected. For example, an excellent place to identify whitepapers on the Internet is by using Google or a specific document hosting site such as Digital Minds (http://www.digital-minds.org/). However, if the target realm is FTP sites, then use File Searching (http://www.filesearching.com/).
   Here is a list of possible search engines to utilze:
   - www.google.com
   - www.altavista.com

- www.dogpile.com
- www.yahoo.com
- www.go.com
- www.filesearching.com
- www.lycos.com
- www.webcrawler.com

These are just a few of the many search engines available. To find others, go to a source such as Google and do a search on the keywords "search engine".

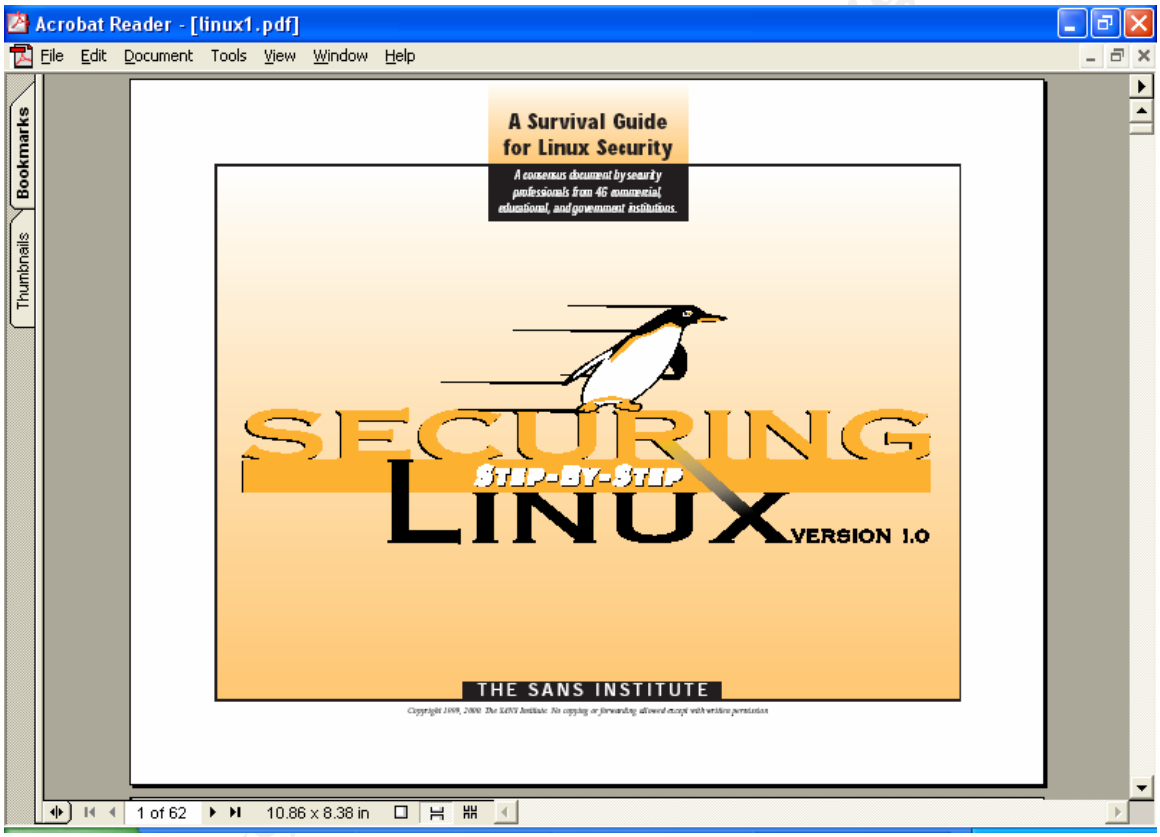
5. Define search criteria based on target realm and tools being utilized. This is where the efforts from step 1 above will begin to pay off. The information gathered in the first step now becomes the list of keywords to be searched for while utilizing tools such as Google. It is important to note that the same search string, such as "ACME DOC", may produce different results based on the search engine in which it is used. So, even though a string does not produce an IP detection with one tool, it may very well produce ten hits in another! Also, the search engine databases are constantly being updated as new information and materials permeate the Internet. Therefore, it is important to periodically recheck a particular search phrase since a search engine that did not produce a detection last week may produce a detection this week with an identical keyword search.

REMEDIATION

At the heart of remediation is the effective and widely used six step incident handling plan. The six steps are *Preparation*, *Identification*, *Containment*, *Eradication*, *Recovery* and *Lessons Learned*. We discussed some of the steps of the Preparation phase in the above *Protection* section. This is what should happen before an IP misuse occurs and if thoroughly done, these proactive efforts will help prevent an IP incident. However, security lapses will occur and the criminal minded will continue to chip away at defenses or exploit any lack of defense.

When an incident does occur, it will be necessary to identify whether or not it is truly your IP. If the misuse in question is plagiarized documents, then the identification may be difficult unless an obvious word-for-word copy was performed. However, as frequently is the case on the Internet, IP will be kept in its nearly original format in plain view. This is what makes plain text searches so successful on the Internet. Identification can usually be done quickly and accurately. Once the IP is identified as being illegally used, then it is time to initiate a containment plan. The main objective is to keep any more damage from being done by this incident. If the misuse is internal, then the containment may involve removing a file from an individual's hard drive. It is a bit more complex if the misuse is external.

Let us examine a recent external incident in which SANS course materials were illegally published on a publicly accessible FTP site. This example will demonstrate *Identification* and *Containment*. The misuse was first identified utilizing the detection method mentioned earlier but with a very powerful file searching tool which searches public FTP sites on the Internet (http://www.filesearching.com). The search string used consisted of only three key words to yield a positive hit. The identified file was a ZIP file containing 19 copyrighted SANS documents. One of the documents was the SANS *Securing Linux Step-by-Step* guide.



Of course, this is very illegal and a big "no-no". The IP was identified to belong to SANS and next it was necessary to identify the location and suspects so that containment could be carried out. This is where public reconnaissance tools come into play. Sam Spade (http://www.samspade.org) was the first tool of choice. Using Sam Spade to do a lookup on the identified domain name yielded a wealth of information on the suspect organization. This tool revealed the Internet Protocol address, city, state, phone, email addresses and individual's names. The SANS IP incident team quickly made a call to the acquired contact information notifying them of their illegal posting. Additionally, a request was made to the company for access logs. The site administrator quickly identified the illegal ZIP file and removed it from their site. The incident was quickly contained and no more damage could be done from that access point.

Additionally, the administrator sent the firewall access logs to the SANS team. This was very valuable information in identifying the extent of the damage.

Log File:

```
[root@bullwinkle /var/log]# grep giac * >giac.txt
 grep: fillup-templates: Is a directory
 grep: iptraf: Is a directory
 grep: samba: Is a directory
 [root@bullwinkle /var/log]# less giac.txt
 all:Aug  5 00:38:24 bullwinkle proftpd[6487]:
bullwinkle.apl.xyz
 (YYYY.XXXX.ZZZZ.net[XX.XX.246.94]) - received: RETR
giac_pdf.zip
all:Aug  5 00:38:24 bullwinkle proftpd[6487]:
bullwinkle.apl.xyz
 (YYYY.XXXX.ZZZZ.net[XX.XX.246.94]) - received: RETR
giac_pdf.zip
 xferlog:Tue Dec 24 17:39:29 2002 128
h158.96.XX.XX.ip.YYYY.net
 8655259 /home/ftp/pub/giac_pdf.zip b_o a XXXX@YYYY.com ftp
0 * c
 xferlog:Thu Dec 26 14:38:38 2002 807 XXXX.YYYY.net 8655259
 /home/ftp/pub/giac_pdf.zip b_o a IEUser@ ftp 0 * c
 xferlog:Fri Dec 27 07:30:19 2002 12 viruswall.apl.xyz
8655259
 /home/ftp/pub/giac_pdf.zip b_o a Administrator@ ftp 0 * c
 xferlog.2:Fri Dec 13 20:22:46 2002 1536 XXXX.kcnet.com
8655259
 /home/ftp/pub/giac_pdf.zip b_o a IEUser@ ftp 0 * c
```

As you can see from the above sanitized log, only a small handful of people accessed the illegal IP. And two of those entries were SANS investigators. This means that from this access point, only one individual downloaded the file according to these log entries. The identification and containment of the IP was a success.

Remediation needs to be methodical, professional and thorough in nature from the beginning phase to the end. Refer to the SANS Computer Security Incident Handling guide for more information on the incident handling phases and other important factors. This guide and others can be purchased via the SANS online store (http://store.sans.org/). Another resource to consider while documenting and preparing for incidents are the SANS Incident Handling forms (http://www.sans.org/incidentforms/). They are a set of general computer security incident forms as well as IP specific incident forms. These forms are also included as an appendix at the end of this document.

CONCLUSION

In conclusion, there are a number of considerations concerning the protection, detection and remediation of IP. IP is a mission critical and valuable component of most organizations. Therefore, individuals and organizations need to increase their ability to provide adequate protection, detection and remediation for IP. This is best achieved by organizations investing in educated and experienced people and by obtaining and maintaining reliable resources. Additionally, people need to be aware of the factors concerning IP. This statement applies to all those involved with IP such as network administrators, end users, and webmasters. Network administrators need to make sure that IP and the hosting systems and resources are properly secured. End users must ensure that they are not making and distributing illegal copies of IP. Even though individuals may feel that their actions are harmless, they are having a direct and negative impact on the effectiveness of organizations and on the economy. Webmasters must take the stance of responsibility as they allow anonymous individuals to post materials on their sites and they need to take reasonable steps to verify that this posted material is not illegal. Thus it is a combined effort to which everyone must contribute. As our world progresses technically, our dependence on digital IP will become greater as will the threats against it.

APPENDIX A: INTELLECTUAL PROPERTY INCIDENT FORMS

The role of documentation in the information security field cannot be over emphasized. Proper incident documentation will have a positive affect on the success of a case should an incident go to court. In a nutshell, documentation should be accurate, detailed, and professional. Keep the material factual and only include information and descriptions that would be appropriate if disclosed in a public courtroom. If it is necessary to include opinions or theories, note them as such. Be meticulous while logging times, keeping communication logs, and documenting procedures followed during the incident handling process. Included in this section is a set of intellectual property incident handling forms that I prepared for the SANS Institute. These may be used in their present form or as a guide to develop more custom fit forms for a specific organization. The forms can also be found online at the SANS web site (http://www.sans.org/incidentforms/).

Intellectual Property Incident Contact List

Date: _____ Page ___ of ___

Intellectual Property (IP) Owner Contacts

Corporate Security Officer:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Corporate Incident Handling, CIRT, or FIRST Team:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Corporate DMCA Agent:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

CIO or Information Systems Security Manager:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Corporate Public Affairs Officer:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Corporate Legal Affairs Officer

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Intellectual Property Incident Contact List

Date: _____ Page ___ of ___

IP Owner Local Contacts

Internet Service Provider Technical Contact:	**Local FBI or Equivalent Agency:**
Name:_____	Name:_____
Title: _____	Title: _____
Phone:_____ Alt. Phone: _____	Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____	Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____	Fax:_____ Alt. Fax:_____
E-mail: _____	E-mail: _____
Address: _____	Address: _____
_____	_____
Local Law Enforcement Computer Crime:	**Local CIRT or FIRST Team:**
Name:_____	Name:_____
Title: _____	Title: _____
Phone:_____ Alt. Phone: _____	Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____	Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____	Fax:_____ Alt. Fax:_____
E-mail: _____	E-mail: _____
Address: _____	Address: _____
_____	_____
Other (Specify):_____	**Other (Specify):_____**
Name:_____	Name:_____
Title: _____	Title: _____
Phone:_____ Alt. Phone: _____	Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____	Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____	Fax:_____ Alt. Fax:_____
E-mail: _____	E-mail: _____
Address: _____	Address: _____
_____	_____

Intellectual Property Incident Contact List

Date: _____ Page ___ of ___

Suspect's Local Contacts

Suspect's Internet Service Provider (ISP) Technical Contact:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Suspect's ISP DMCA Agent:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Suspect's Local FBI or Equivalent Agency:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Suspect's Local Law Enforcement Computer Crime:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Suspect's Local CIRT or FIRST Team:

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Other (Specify):_____

Name:_____

Title: _____

Phone:_____ Alt. Phone: _____

Mobile: _____ Pager:_____

Fax:_____ Alt. Fax:_____

E-mail: _____

Address: _____

_____

Intellectual Property Incident Contact List

Date: _____ Page ___ of ___

Suspect's Local Contacts

Suspect's Web Hosting Technical Contact:	**Suspect's Web Hosting DMCA Agent:**
Name:_____	Name:_____
Title: _____	Title: _____
Phone:_____ Alt. Phone: _____	Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____	Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____	Fax:_____ Alt. Fax:_____
E-mail: _____	E-mail: _____
Address: _____	Address: _____
_____	_____
Other (Specify):_____	**Other (Specify):_____**
Name:_____	Name:_____
Title: _____	Title: _____
Phone:_____ Alt. Phone:_____	Phone:_____ Alt. Phone:_____
Mobile:_____ Pager:_____	Mobile:_____ Pager:_____
Fax:_____ Alt. Fax:_____	Fax:_____ Alt. Fax:_____
E-mail:_____	E-mail:_____
Address:_____	Address:_____
_____	_____
Other (Specify):_____	**Other (Specify):_____**
Name:_____	Name:_____
Title: _____	Title: _____
Phone:_____ Alt. Phone: _____	Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____	Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____	Fax:_____ Alt. Fax:_____
E-mail: _____	E-mail: _____
Address: _____	Address: _____
_____	_____

Intellectual Property Incident Contact List

Date: _____ Page ___ of ___

Suspect Contacts

Suspect Individual:	**Suspect Organization:**
Name:_____	Name:_____
Title: _____	Title: _____
Phone:_____ Alt. Phone: _____	Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____	Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____	Fax:_____ Alt. Fax:_____
E-mail: _____	E-mail: _____
Address: _____	Address: _____
_____	_____
Suspect Technical Contact:	**Suspect DMCA Agent:**
Name:_____	Name:_____
Title: _____	Title: _____
Phone:_____ Alt. Phone: _____	Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____	Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____	Fax:_____ Alt. Fax:_____
E-mail: _____	E-mail: _____
Address: _____	Address: _____
_____	_____
Suspect Legal Contact:	**Other (Specify):_____**
Name:_____	Name:_____
Title: _____	Title: _____
Phone:_____ Alt. Phone: _____	Phone:_____ Alt. Phone: _____
Mobile: _____ Pager:_____	Mobile: _____ Pager:_____
Fax:_____ Alt. Fax:_____	Fax:_____ Alt. Fax:_____
E-mail: _____	E-mail: _____
Address: _____	Address: _____
_____	_____

Intellectual Property Incident Identification

Date: _____ Page ___ of ___

General Information

Incident Detector's Information:

Name:_____ Date and Time Detected: _____

Title: _____

Phone:_____ Alt. Phone: _____ Location Incident Detected From: _____

Mobile: _____ Pager:_____ _____

Fax:_____ Alt. Fax:_____ Additional Information:_____

E-mail: _____ _____

Address: _____ _____

_____ _____

Detector's Signature:_____ Date Signed: _____

Intellectual Property Profile Summary

Type of Intellectual Property (IP) Detected: Total Number of IP Items Detected: _____

☐ Document(s) ☐ Audio ☐ Application(s)
☐ Image(s) ☐ Video

Additional Information:_____

Other:_____ _____

Root Location of IP Items (URL, etc) on Detected System:_____

_____

How was the Intellectual Property Detected:_____

_____

_____

_____

_____

_____

_____

_____

Intellectual Property Incident Identification

Date: _____ Page ___ of ___

Intellectual Property Profile Detail – Detected Items Log

IP Item Number: _____ **File Type: _____** **Size: _____**

Filename:_____ Time Stamp: _____ Version:_____

Detected File Location (URL, etc.):_____

Original File Location (URL, etc.):_____

Title:_____ Copyright:_____

Author:_____ Author E-mail:_____

Publisher:_____ Publish Date:_____

Company:_____ Company E-mail:_____

Company Address:_____ Company Phone:_____ Fax:_____

Additional Information:_____

_____

IP Item Number: _____ **File Type: _____** **Size: _____**

Filename:_____ Time Stamp: _____ Version:_____

Detected File Location (URL, etc.): _____

Original File Location (URL, etc.): _____

Title:_____ Copyright:_____

Author:_____ Author E-mail:_____

Publisher:_____ Publish Date:_____

Company:_____ Company E-mail:_____

Company Address:_____ Company Phone:_____ Fax:_____

Additional Information:_____

_____

Intellectual Property Incident Containment

Date: _____ Page ___ of ___

How were the intellectual property items compromised:

Are the original files accessible from company resources? ☐ YES ☐ NO

If YES, properly document location(s) on the Incident Identification form.

Are the original files secured? ☐ YES ☐ NO

If YES, how and where are these files secured: _____

Have the company systems been reviewed for possible authorized or unauthorized access? ☐ YES ☐ NO

If YES, where is the location of the report or incident handling forms documenting this access: _____

_____

If NO, what was the reason:_____

_____

Have trusted partner systems been reviewed for possible authorized or unauthorized access? ☐ YES ☐ NO

If YES, where is the location of the report or incident handling forms documenting this access: _____

_____

If NO, what was the reason:_____

_____

Are the trusted partner system files secured? ☐ YES ☐ NO

If YES, how and where are these files secured:_____

_____

If NO, what was the reason: _____

_____

List other known authorized and unauthorized mechanisms of file distribution and possible usage or exploitation:

_____

_____

_____

_____

_____

_____

Intellectual Property Incident Eradication

Date: _____ Page ___ of ___

Names and Contact information of all people performing forensic and investigational duties:

_____

_____

_____

_____

_____

_____

_____

Was the vulnerability identified? ☐ YES ☐ NO

If YES, describe: _____

_____

_____

_____

Was the vulnerability eradicated? ☐ YES ☐ NO

If YES, describe: _____

_____

_____

_____

_____

What were the validation procedures used to ensure the problem was eradicated: _____

_____

_____

_____

_____

_____

Incident Communication Log

Date: ________ Page ___ of ___

Date:______________ Time:_________ ☐ am ☐ pm Method (mail, phone, email, etc.):_______________

Initiator Name:________________________________ Receiver Name:________________________________

Initiator Title: _________________________________ Receiver Title: _________________________________

Initiator Organization: __________________________ Receiver Organization:___________________________

Initiator Contact Info:___________________________ Receiver Contact Info: ___________________________

Details:____

____

____

____

Date:______________ Time:_________ ☐ am ☐ pm Method (mail, phone, email, etc.):_______________

Initiator Name:________________________________ Receiver Name:________________________________

Initiator Title: _________________________________ Receiver Title: _________________________________

Initiator Organization: __________________________ Receiver Organization:___________________________

Initiator Contact Info:___________________________ Receiver Contact Info: ___________________________

Details:____

____

____

____

Date:______________ Time:_________ ☐ am ☐ pm Method (mail, phone, email, etc.):_______________

Initiator Name:________________________________ Receiver Name:________________________________

Initiator Title: _________________________________ Receiver Title: _________________________________

Initiator Organization: __________________________ Receiver Organization:___________________________

Initiator Contact Info:___________________________ Receiver Contact Info: ___________________________

Details:____

____

____

____

REFERENCES & ADDITIONAL RESOURCES

Northcutt, Stephen. SANS Computer Security Incident Handling Step-by-Step Guide, The SANS Institute, 2003.

Poltorak, Alexander I. and Paul J. Lerner. Essentials of Intellectual Property. John Wiley & Sons, Inc., 2002.

SANS Web Site
http://www.sans.org

Federal Cyber Crime Informational Site
http://www.cybercrime.gov

U.S. Patent & Trademark Office
http://www.uspto.gov

United States Copyright Office
http://lcweb.loc.gov/copyright/

World Intellectual Property Organization
http://www.wipo.org/index.html.en

The Digital Millennium Copyright Act of 1998
http://www.loc.gov/copyright/legislation/dmca.pdf

Pretty Good Privacy
http://www.pgp.com

Snort Intrusion Detection System
http://www.snort.org

Google Search Engine
http://www.google.com

FTP Directory Search Engine
http://www.filesearching.com